METHOD AND DEVICE FOR PROTECTING INTEGRATED CIRCUITS AGAINST PIRACY

Field of the Invention

This invention relates to methods and devices for protecting an integrated circuit against piracy, at least when the circuit performs operations that involve reading confidential data stored within the integrated circuit.

Background of the Invention

Conventionally, electronic transactions carried-out on a terminal via a smart card are protected via an authentication procedure for the card, which involves an encryption algorithm. During such an authentication procedure, a terminal sends a random code to the card, and the smart card must respond by generating an authentication code, which is transformed into a random code by the encryption algorithm. The terminal calculates, on its side, the transformed random code and compares the obtained result with the one sent by the card. If the authentication code sent by the card is valid, the transaction is authorized.

In a smart card integrated circuit, an encryption algorithm is generally executed by a hard-wired logic circuit, or an encryption coprocessor, to

which is attributed a secret key or an encryption key, which is stored within a protected area of the integrated circuit memory. It is therefore essential to guarantee an absolute protection of this secret key, since the encryption algorithms implemented within the authentication procedures are well known and only the secret key guarantees the tamperproof character of the authentication procedure.

However, in recent years, techniques for pirating of integrated circuits have considerably improved and nowadays involve sophisticated analysis methods based on the observation of the current used by the elements in the integrated circuit during the execution of confidential operations. Presently, there are two types of methods for analyzing the current used, namely the SPA analysis methods (Single Power Analysis) and the DPA analysis methods (Differential Power Analysis). DPA analysis methods, which are more efficient than the former methods, allow a secret key to be revealed via a single observation of changes in the current used by the encryption circuit, without having to read the data flowing in the integrated circuit internal bus and to identify the memories that are read. Such a method relies upon a correlation of samples of the current used with a mathematical model of the encryption circuit and assumptions about the secret key's value. The correlation allows the dc-component in the used current to be suppressed and consumption peaks to be revealed which show the operation performed by the encryption circuit and confidential data values. With such a method, only about 1000 samples need to be recorded for a DES secret key to be obtained.

To counteract such piracy methods, various countermeasure methods have been suggested that allow variations in the power consumption to be hidden or scrambled, at least during the execution of confidential operations. Such countermeasures only allow increasing the number of necessary samples up to 200,000 which can still be reached by automating measurements.

Summary of the Invention

Accordingly, an object of the present invention is to provide integrated circuits designed to handle confidential information, in particular those that are mounted within smart cards with an additional protection.

This object is achieved by providing a method for protecting an integrated circuit against piracy, including the following successive steps performed by the integrated circuit before a predetermined processing sequence: detecting the state of at least one timer, controlling the activation of the timer if it is not activated, and disabling the integrated circuit if the timer is activated.

According to one feature of the invention, this method further comprises the step, performed by the integrated circuit if the predetermined processing sequence has been performed normally, of deactivating the timer.

According to another feature of the invention, this method further comprises the step, performed by the integrated circuit if it is detected that the timer is activated, of modifying the value of a counter within a protected area in a non-volatile

memory, comparing the value of this counter to a predefined threshold, and performing a processing for protecting confidential data stored within memories in the integrated circuit if the counted value reaches a predefined threshold.

Advantageously, said protection processing includes erasing the confidential data from the memories in integrated circuit. Specifically, the protection processing includes erasing a secret code stored within a memory in the integrated circuit. Alternatively, the protection processing includes erasing all memories in the integrated circuit.

Before executing a calculation in a sequence comprising a predefined number of calculations, the integrated circuit preferably detects the state of a respective timer, each calculation being respectively associated with one timer, controls the activation of the associated timer if it is not activated, and disables itself if the associated timer is activated. This invention also relates to an integrated circuit protected against piracy, and including at least one timer circuit comprising an activation device for activating a timer adapted to remain in the activated state as long as the circuit is powered-on and for a predetermined duration if the circuit is powered-off. Also, the integrated circuit includes a deactivating device deactivating the timer. The activated or deactivated state of the timer is also detected. The integrated circuit further includes a timer reader for reading the state of the timer, and for disabling the integrated circuit at predefined time points if the timer is in the activated state.

According to a feature of this invention, the integrated circuit deactivates the timer after a normal execution of a predetermined processing sequence.

Advantageously, each timer circuit detects the presence of a supply voltage, and allows the activation or deactivation of the timer when the supply voltage is detected as present during the predetermined time period.

According to another feature of this invention, the integrated circuit comprises several timer circuits, each timer circuit being associated with a calculation performed by the integrated circuit, the integrated circuit determining, before each calculation, the state of the timer associated with the calculation, activating the associated timer if it is not activated and disabling itself if the associated timer is activated.

Preferably, each timer circuit comprises a capacitor associated with: a discharge circuit designed so that the capacitor slowly discharges when the device is powered-off, a circuit for detecting capacitor charging, a capacitor charging controlling device, and capacitor discharging controlling device. Advantageously, capacitor discharging controlling device is designed for discharging the capacitor more rapidly than when the device is powered off.

According to yet another feature of this invention, the integrated circuit comprises a MOS transistor having very small leakage currents, which is associated with the capacitor, so that it is only discharged by the leakage currents when the integrated circuit is powered-off. Preferably, it also comprises

a test circuit, which is controlled by a test control command, for reducing the timing period.

Brief Description of the Drawings

These and other objets, features and advantages of the present invention will become more apparent upon a consideration of the following description of a preferred embodiment of the invention, disclosed by way of non-limiting example in reference to the accompanying drawings, in which :

Fig. 1 is a schematic diagram showing an integrated circuit according to the invention, communicating with a terminal.

Fig. 2 is a more detailed schematic diagram of an example of the protection device according to the present invention, provided within the integrated circuit shown in Fig. 1.

Fig. 2a is a more detailed schematic diagram of a circuit element in the device shown in Fig. 2.

Figs. 3a to 3e are timing diagrams showing curves of electrical signals as a function of time illustrating the operation of the circuits shown in Figs. 2 and 2a.

Figs. 4a to 4d are timing diagrams showing other curves of electrical signals as a function of time illustrating the operation of the circuits shown in Figs. 2 and 2a, when the circuits are successively powered-off and then powered-on.

Figs. 5a to 5f are timing diagrams showing curves of electrical signals as a function of time illustrating the overall operation of the circuit shown in Fig. 2.

Figs. 6a to 6d are timing diagrams showing curves of electrical signals as a function of time illustrating the overall operation of the circuit shown in Fig. 2, in the case when the circuit is powered back on after a malfunction is detected.

Figs. 7A to 7d are timing diagrams showing curves of electrical signals as a function of time illustrating the overall operation of a modification of the integrated circuit according to this invention.

Detailed Description of the Preferred Embodiments

Fig. 1 diagrammatically shows the construction of an integrated circuit 1 for smart cards. This integrated circuit 1 comprises a central processor unit 2, for example a microprocessor or microcontroller, a communication unit 7 enabling communications with an external terminal 10, an encryption circuit 6 and memories 4, namely a read only memory in which is stored the operating system of CPU 2, a RAM memory for storing temporary data, and a programmable and erasable memory, for example an EEPROM, for storing one or more application programs. CPU 2, memories 4, encryption circuits 6, and communication unit 7 are interconnected through a common data bus 3.

A secret key used by the encryption circuit 6 is stored within a protected area in the ROM or EEPROM memory. The integrated circuit may also comprise a countermeasure circuit 8 designed for scrambling a DPA analysis. According to the invention, the integrated circuit 1 also comprises a timer circuit 5 for more efficiently resisting a DPA attack (Differential Power Analysis).

In Fig. 2, this circuit 5 comprises a timer circuit, which includes an nMOS transistor M1 advantageously designed to have a very small drain-source leakage current, i.e. of minimum drain perimeter and surface. This transistor has its drain connected to the ground through another nMOS transistor 27, the gate of which is coupled to a discharge control input Dchrg. The drain of transistor M1 is also coupled through a diode D1 reverse-connected to the drain of a pMOS transistor 24 having its source coupled to the voltage source V_{dd}. The gate of transistor 24 is connected to the output of an inverter 25 whose input is connected to the output of an OR gate 23. This OR gate 23 has a first input connected to the charge control input Chrg of circuit 5, and a second input connected to output Q of circuit 5.

Thus, if output Q or charge control input Chrg is at logic level 1, the source of the transistor goes to logic level 1. Conversely, if Q and Chrg are at logic level 0, the drain of transistor M1 is isolated through diode D1, which is then in the off-state. This diode is preferably of the isolation well type, so as to be isolated from the substrate (i.e. the ground) on which is formed transistor M1, to reduce leakage currents.

Additionally, the source of transistor M1 is connected, on the one hand, to the ground through a capacitor C, and on the other hand, to output Q of circuit 5 through two series-connected inverter stages for transforming the voltage across capacitor C into a logic signal. Conventionally, each inverter stage comprises a pMOS transistor 20, 30, and an nMOS transistor 29, 31, which are series-connected between

voltage source V_{dd} and the ground. Transistors 21 to 31 are constructed so that a very small voltage across the capacitor provides a logic level 1 at output Q.

In addition, the gate of transistor M1 is connected to the output of an AND gate 22 whose inputs are connected to a circuit 32 for detecting supply voltage V_{dd} and to the output of an OR gate 21, respectively. The OR gate 21 comprises three input channels, namely a first channel connected to output Q, a second channel connected to the charge control input Chrg, and a third channel connected to the discharge control input Dchrg.

Fig. 2a gives a detailed view of circuit 32 for detecting supply voltage V_{dd}. This circuit comprises two diode-connected pMOS transistors 35, 36 (with a gate-drain connection), both of these transistors being series-connected between voltage supply V_{dd} and the drain of an nMOS transistor 37 having its gate connected to supply voltage V_{dd} and its source connected to the ground, so as to act as a resistor. The junction between transistors 36 and 37 is connected to a first inverter stage comprising a pMOS transistor 38 having its source at potential V_{dd} and an nMOS transistor 39 having its source connected to the ground, and this junction is connected to the gates of both transistors 38 and 39. The junction between drains of transistors 38 and 39 is connected to a capacitor 40 having its other terminal connected to the ground, and to a second inverter stage comprising a pMOS transistor 41 with its source at potential V_{dd}, and an nMOS transistor 42 having its source connected to the ground, the junction between the drains of both transistors 41, 42 providing an Enable output signal of circuit 32. In fact, the

assembly comprising capacitor 40 and the last inverter stage with transistors 41 and 42 acts as a delay line. The operation of circuit 5 will now be explained in more detail referring to Figs. 3 and 4, which show various signals in the integrated circuit 1 change as a function of time.

As shown in Figs. 3a to 3e, when the circuit supply voltage V_{dd} reaches a value $2V_{TP}$, where V_{TP} is the ON voltage of each transistor 35, 36, signal Enable goes from low to high level after a given time delay D corresponding to the charging time of capacitor 40 (Figs. 3a and 3b). Conversely, when voltage V_{dd} decreases below $2V_{TP}$, transistors 35 and 36 are turn off, so that signal Enable goes low.

To control the charging of capacitor C, CPU 2 sends a pulse at the charge input Chrg of circuit 5 (see curve in Fig. 3c), signal Enable being high. As a result, the output of OR gate 21 goes high, as well as the output of AND gate 22. A voltage is then applied to the gate of transistor M1. Similarly, the output of OR gate 23 goes high, so that transistor 24 is turned on. The circuit supply voltage V_{dd} is then applied to the drain of transistor M1, which is then on the ON state, transistor 27 being in the OFF state (with discharge command Dchrg set to 0), thus isolating the drain of transistor M1 from the ground. As a result, capacitor C charges as shown by the curve in Fig. 3d. As soon as the voltage across capacitor C becomes greater than gate voltage V_{TH} that turns transistor 29 ON, with transistor 28 in the OFF-state, transistor 32 turns ON, so that output Q goes to logic level 1 (curve in Fig. 3e), which then continues the action of the charge pulse to maintain transistor M1 in the ON-state. The

charge control pulse is thus chosen to be sufficiently long for the voltage across capacitor C to reach at least value V_{TH}.

Conversely, if the circuit is powered OFF, Enable signal goes low, so that the output of AND gate 22 goes low, which turns transistor M1 OFF. Therefore, capacitor C is no longer supplied with a voltage and discharges through the drain of transistor M1 (through the leakage current from the drain-substrate diode in the transistor). When the circuit is non longer powered, output Q follows supply voltage V_{DD} and therefore falls to 0. As long as time Δt, corresponding to the capacitor discharge circuit time constant has not elapsed, the voltage across capacitor C remains greater than threshold voltage V_{TH}. As a consequence, as shown in Figs. 4a to 4d, whenever the circuit is powered back on before time Δt has elapsed, transistors 28 and 30 become powered on and therefore so that output Q rises again and capacitor C automatically recharges.

Within circuit 5, the time constant Δt is the time period during which the integrated circuit 1 has to be powered-off for capacitor C to discharge. The value of Δt can be obtained from the following formula:

$$\Delta t = \frac{C\Delta V}{i} \quad (1)$$

where C is the capacitance of capacitor C, ΔV is the voltage change across the capacitor during time Δt and i is the discharge current.

If the power supply V_{dd} of the integrated circuit is stopped, capacitor C slowly discharges

because of the very small leakage currents which flow through transistor M1. As a consequence, even if the capacitance of capacitor C is very small, namely a few pF, the voltage across capacitor C remains greater than the triggering threshold of the inverter stages during time period Δt.

Within an MOS component, C can be 10 pF, ΔV can be 2V, and I can be 10 pA. Under these conditions, the time constant Δt equals 2 secs. Typically, with MOS technology, this time constant can be as high as 5 secs. To increase time constant Δt, several capacitors can advantageously be connected in parallel.

If, while capacitor C charges, CPU 2 sends a pulse on the discharge input Dchrg, transistor 27 turns on, which connects drain of transistor M1 to the ground, so that capacitor C then discharges nearly instantaneously, both transistor M1 and 27 having a small resistance in the ON-state.

During a very short time period, it can be seen that the voltage source V_{dd} is directly connected to the ground through transistor 27, diode D1 and transistor 24. This electrical mismatch is solved by overdimensioning transistor 27 and by making transistor 24 resistive (by reducing its size). In fact, this mismatch will last as long as capacitor C discharges and causes output Q to switch.

As soon as the voltage across capacitor C again falls below V_{TH}, transistor 28 turns on, whereas transistor 29 turns off. Transistor 30 then in turn switches to the off-state, whereas transistor 31 switches to the on state, so that output Q is connected to the ground and thus goes to logic level 0.

The length of discharge control pulse Dchrg should also be larger than the discharge time of capacitor C through transistors M1 and 27, until V_{TH} is reached. It should be noted that the discharge control command is applied to OR gate 21 so as to make sure that capacitor C discharges entirely. Without this provision, the discharging of capacitor could be stopped as soon as this voltage again falls below voltage V_{TH}, time from which signal Q goes low again, which would disable gate 21 and therefore transistor M1.

Fig. 5a shows the change in voltage V_{dd} during a transaction established with the integrated circuit. Slightly after the integrated circuit is powered-on, the reset signal shown in Fig. 5b goes from logic level 0 to logic level 1, which causes an initialization process carried-out by CPU 2, and then a series of n authentication calculations, as can be seen in Fig. 5c, which shows the activity of CPU 2. After these n calculations have been performed, if they result in terminal 10 being authenticated, the CPU starts a normal operating session for performing the transaction requested by the terminal.

In normal operation, output Q (curve in Fig. 5d) is low when the circuit is powered-on. At the end of the initialization procedure, circuit 5 is controlled at time point t1 by CPU 2 which sends a pulse to input Chrg, so as to cause capacitor C to charge, therefore making output Q high, whereas Enable signal is high. As soon as the voltage across capacitor reaches V_{TH}, output Q goes low, so that the gate and source voltages of transistor M1 are maintained at high

level. Capacitor C therefore remains charged and signal Q is maintained at high level.

If the authentication calculations (Fig. 5c) result in the terminal being authenticated, CPU 2 controls the discharging of capacitor C by sending a pulse on the discharged control input Dchrg, and output Q again goes low at time point t2. On the contrary, if, during the authentication calculations, CPU 2 detects abnormal operation due to a piracy attempt, it does not perform a capacitor discharge control, for example, within an idling loop (Figs. 5e, 5f).

If, thereafter, an attempt is made to reset circuit 1 by powering it off for a short duration smaller than the discharge time of capacitor C, CPU 2, which executes the initialization procedure, detects that signal Q is still high, which indicates that capacitor C is not entirely discharged and disables itself (Fig. 6c). Therefore, to entirely reinitialize circuit 1, it is necessary to wait for at least Δt, so that the component can be restarted under normal conditions.

During a DPA analysis of the integrated circuit, therefore, it is necessary to wait until capacitor C is discharged between each acquisition sequence of current measurement samples, which considerably lengthens the time taken to carry-out such an analysis.

To entirely suppress the possibility that such an analysis be performed, a provision can be made so that, before each disabling operation, CPU 2 increments a disable counter stored within the EEPROM memory and indefinitely disables itself when the counted value reaches or exceeds some predefined

threshold. The indefinite disabling of the integrated circuit can for example include erasing the secret key that is stored within the EEPROM memory, or more generally, in erasing all confidential data stored within this memory, or else, the whole contents thereof.

A further provision can also be to connect the drain of transistor M1 to an nMOS transistor 26 having its gate connected to a test control input and its source connected to a circuit 31 comprising a plurality of nMOS transistors connected in parallel between the source of transistor 26 and the ground, these transistors being connected in the off-state (with their gate grounded). These transistors have the same size as transistor M1, so that the leakage current which discharges capacitance C is n times greater than that of M1, where n is the number of transistors in circuit 33. This circuit 33 therefore allows time constant Δt = RC of the timer circuit to be reduced to a value that will allow tests to be performed on integrated circuit 1 (where R corresponds to the resistance of circuit 33 and C is the capacitance of capacitor C).

Of course, the test command should be made sufficiently inaccessible so that it could not be executed by possible pirates.

According to a modification of the present invention, several timer circuits 5 can be provided within integrated circuit 1, such as one circuit per authentication calculation sequence. As shown in Figs. 7a to 7d, instead of instructing the charging of capacitor C during the initialization sequence performed by CPU 2, each calculation sequence comprises

an instruction to read the value of output signal Qi from the associated timer circuit 5 and then, if this signal is high, an instruction to discharge the capacitor in this circuit, so as to make signal i high, as shown in Figs. 7b to 7d.

In this way, if the same calculation sequence is requested twice during the same authentication procedure without powering-off circuit 1 for a sufficient time period, CPU 2 detects it by reading the value of signal Qi corresponding to the calculation sequence, and disables itself.